CLAIMS

1. A method for providing an application to be executed on a device, the device being arranged with a secure environment to which access is strictly controlled by a device processor, the method comprising:

providing the device (201) with an encrypted application (204);

providing, via a secure channel (207) into the secure environment (205), the device (201) with a first key for decrypting said encrypted application (204);

decrypting, in the secure environment (205), said encrypted application (204) by means of said first key;

re-encrypting, in said secure environment, the application (209) by means of a second key; and

storing, outside said secure environment, the re-encrypted application.

2. A method for providing an application to be executed on a device, the device being arranged with a secure environment to which access is strictly controlled by a device processor, the method comprising:

providing the device (201) with an encrypted application (204);

providing, via a secure channel (207) into the secure environment (205), the device (201) with a first key for decrypting said encrypted application (204);

encrypting, in said secure environment (205), said first key by means of a second key; and

storing, outside said secure environment (205), the encrypted first key.

3. The method according to claim 1, the method comprising:

encrypting, in said secure environment (205), said first key by means of the second key; and

storing, outside said secure environment (205), the encrypted first key.

4. The method according to claim 1, wherein said second key is symmetric and can be derived from the application (202).

5. The method according to claim 4, wherein said second key is comprised in the application (202) itself.

6. The method according to claim 4, wherein said second key is generated in the secure environment (205) using an application seed.

7. The method according to claim 1, wherein multiple keys can be transferred successively on the secure channel into the secure environment, each key being used to decrypt a corresponding encrypted application in the secure environment.

8. A system arranged to provide an application to be executed on a device, the device being arranged with a secure environment to which access is controlled by a device processor, the system comprising:

means for providing the device (201) with an encrypted application (204);

means for providing, via a secure channel (207) into the secure environment (205), the device (201) with a first key for decrypting said encrypted application (204);

means for decrypting, in the secure environment (205), said encrypted application (204) by means of said first key;

means for re-encrypting, in said secure environment, the application (209) by means of a second key; and

means for storing, outside said secure environment, the re-encrypted application.

9. A system arranged to provide an application to be executed on a device, the device being arranged with a secure environment to which access is controlled by a device processor, the system comprising:

means for providing the device (201) with an encrypted application (204);

means for providing, via a secure channel (207) into the secure environment (205), the device (201) with a first key for decrypting said encrypted application (204);

means for encrypting, in said secure environment (205), said first key by means of a second key; and

means for storing, outside said secure environment (205), the encrypted first key.

10. The system according to claim 8, the system comprising:

means for encrypting, in said secure environment (205), said first key by means of the second key; and

means for storing, outside said secure environment (205), the encrypted first key.

11. The system according to claim 8, wherein said second key is symmetric and can be derived from the application (202).

12. The system according to claim 11, wherein said second key is comprised in the application (202) itself.

13. The system according to claim 11, wherein said second key is generated in the secure environment (205) using an application seed.

14. The system according to claim 8, wherein the system is arranged such that multiple keys can be transferred successively on the secure channel into the secure environment, each key being used to decrypt a

corresponding encrypted application in the secure environment.

15. The method of claim 2, wherein said second key is symmetric and can be derived from the application (202).

16. The method of claim 15, wherein said second key is comprised in the application (202) itself.

17. The method of claim 15, wherein said second key is generated in the secure environment (205) using an application seed.

18. The method of claim 2, wherein multiple keys can be transferred successively on the secure channel into the secure environment, each key being used to decrypt a corresponding encrypted application in the secure environment.

19. The method of claim 9, wherein said second key is symmetric and can be derived from the application (202).

20. The method of claim 19, wherein said second key is comprised in the application (202) itself.

21. The method of claim 9, wherein the system is arranged such that multiple keys can be transferred successively on the secure channel into the secure environment, each key being used to decrypt a corresponding encrypted application in the secure environment.